Risk Management Agency
USDA

Privacy Impact Assessment

For

Windows General Support System

March 2007

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the System. This document has been completed in accordance with the requirements of the E-Government Act of 2002.

MANAGEMENT CERTIFICATION – Please check the appropriate statement.

_____ The document is accepted.

_____ The document is accepted pending the changes noted.

_____ The document is not accepted.

_____ **We** fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

_____	_____
System Manager	DATE
_____	_____
OCIO/Project Representative	DATE
_____	_____
Program/Office Head	DATE
_____	_____
OCIO	DATE
_____	_____
Chief FOI/PA	DATE
_____	_____
Senior Official for Privacy	DATE

Name of Project: Windows General Support System
Program Office:
Project's Unique ID:

A. CONTACT INFORMATION:

1. Who is the person completing this document?

Eric Baer, ISSPM
Risk Management Agency, Kansas City
(816) 823-1950
eric.baer@rma.usda.gov

2. Who is the system owner?

Vondie O'Conner, CIO
Risk Management Agency, Kansas City
(816) 823-4459
Vondie@rma.usda.gov

3. Who is the system manager for this system or application?

Chief, SAB
Risk Management Agency, Kansas City

4. Who is the IT Security Manager who reviewed this document?

See #1

5. Did the Chief FOI/PA review this document?

Terrie Ray, FOI Specialist
Risk Management Agency, WDC

terrie.ray@rma.usda.gov

6. Did the Agency's Senior Officer for Privacy review this document?

Yes, see #2

7. Who is the Reviewing Official?

See #2.

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1. Does this system contain any information about individuals?

(a) Is this information identifiable to the individual?

Yes

(b) Is the information about individual members of the public?

Yes

(c) Is the information about employees?

Yes

2. What is the purpose of the system/application?

This is a back office system that supports the day to day operation and delivery of the Federal Crop Insurance Program. While this is not the primary RMA business system, the Windows GSS does support collaboration, file storage, and messaging.

3. What legal authority authorizes the purchase or development of this system/application?

Authority to purchase/operate this system stems from the Federal Crop Insurance Act which authorizes RMA to administer the Federal Crop Insurance Program.

C. DATA in the SYSTEM:

1. Generally describe the type of information to be used in the system and what categories of individuals are covered in the system?

On the whole, the information in the system is innocuous office automation type information. However, the information stored that is privacy information is information regarding crop insurance policies and compliance activities. Additionally, it is likely that personnel data about employees performance, disciplinary activities, and other personnel information is on the system.

2. What are the sources of the information in the system?

(a) Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

The source of the information comes from the Approved Insurance Providers, which is collected for the Federal Crop Insurance Program by their agents and contractors. Information about employees comes either directly from the individual or their supervisor.

(b) What Federal agencies are providing data for use in the system?

RMA only

(c) What State and local agencies are providing data for use in the system?

none

(d) From what other third party sources will data be collected?

Approved Insurance Providers under the terms of the Standard Reinsurance Agreement and the Federal Crop Insurance Program

(e) What information will be collected from the employee and the public?

The primary information that is collected is policy information, which includes the name, taxID (or SSN), address, and farming information. Employee data can include name, performance data, and possibly the SSN.

3. Accuracy, Timeliness, and Reliability

(a) How will data collected from sources other than USDA records be verified for accuracy?

In order for the crop insurance policies to be active, their data must be valid. Most of the PII data on the Windows GSS is derivative from the business systems, which have a built in checking mechanism.

(b) How will data be checked for completeness?

See above statement.

(c) Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

(d) Are the data elements described in detail and documented? If yes, what is the name of the document?

D. ATTRIBUTES OF THE DATA:

1. **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

Yes. The PII is required for participation in the Federal Crop Insurance Program. Employee data is collected for ordinary business purposes.

2. **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

This system will not derive any new data from the information collected.

3. **Will the new data be placed in the individual's record?**

N/A. See above

4. **Can the system make determinations about employees/public that would not be possible without the new data?**

N/A

5. **How will the new data be verified for relevance and accuracy?**

N/A

6. **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

Currently, access list exist on all the data that will prevent internal misuse or mishandling. A pilot program is underway to encrypt all USB drives that can attach to the system. Additionally, an evaluation program for encryption of the hard drives of mobile computers is ongoing.

7. **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?** Explain.

8. **How will the data be retrieved?**

The most common personal identifier that is used is last name.

9. **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

For members of the public, the type of reports produced are those required to audit insurance companies or individuals for compliance with the crop insurance program.

Employees will have reports that relate to their performance generated by their supervisors.

10. What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses and how individuals can grant consent.)

The SSN is required for participation in the Federal Crop Insurance Program. Each individual participating in the Program is given a copy of the Privacy Act statement that outlines their rights under statute.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The Windows GSS falls under the management of the Chief of the Systems Administration Branch. Additionally, the controls are specified through a central repository (Group Policy) and pushed to all nodes in the network.

2. What are the retention periods of data in this system?

As of 28 March 2007, indefinite.

3. What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Disposition of logical data is a simple matter of deleting the file. Standard use of the operating system will ensure no remnants remain. Disposition of a system is accomplished by the security staff. They use a method that wipes the drive a minimum of 5 times, the writes over the disk in a random pattern of 1s and 0s.

4. Is the system using technologies in ways that the USDA has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No

5. How does the use of this technology affect public/employee privacy?

This technology will not adversely affect privacy, as the information would be maintained in hard copy if it did not exist.

6. Will this system provide the capability to identify, locate, and monitor

individuals? If yes, explain.

No. This system is only used as a back office repository and collaboration tool.

7. **What kinds of information are collected as a function of the monitoring of individuals?**

N/A

8. **What controls will be used to prevent unauthorized monitoring?**

N/A

9. **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

FCIC-2: Compliance Review Cases
FCIC-6: List of Ineligible Producers

10. **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

Yes. This system is set to take on the majority of RMA's business processing. This particular application is still in the design phase, and the appropriate documentation will be prepared when this system is further along.

F. ACCESS TO DATA:

1. **Who will have access to the data in the system?**

System Administrators (contractors, they may not have explicit access, but as system administrators, they can get access). Users and managers (usually only the person that created the file and their immediate co-workers and managers).

2. **How is access to the data by a user determined?**

This access is determined by job function.

3. **Will users have access to all data on the system or will the user's access be restricted? Explain.**

Access is restricted on a job function or need-to-know basis.

4. **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** (Please list processes and training materials)

Users are reminded that access is granted on a need to know basis.

5. **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system**?

Yes. Privacy and non-disclosure clauses are included in the contract.

6. **Do other systems share data or have access to the data in the system? If yes, explain.**

No. This system does not share with external entities. The Magnum and CIMS Applications are excluded, as they have their own Privacy Impact Assessment.

7. **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

N/A

8. **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?**

The Ineligible list is shared with the Department of the Treasury, but there is not a direct interface.

9. **How will the data be used by the other agency?**

This data is used to collect debts owed the Federal Government.

10. **Who is responsible for assuring proper use of the data?**

Department of the Treasury

APPENDIX A
DECLARATION OF PRIVACY PRINCIPLES

The privacy principles set forth in this declaration are based on the ethical and legal obligations of the United States Department of Agriculture to the public and are the responsibility of all USDA employees to recognize and treat their office as a public trust.

The obligation to protect client and partner privacy and to safeguard the information clients and partners entrust to us is a fundamental part of the USDA's mission to administer the law fairly and efficiently. Clients and partners have the right to expect that the information they provide will be safeguarded and used only in accordance with law. In recognition of these obligations, policies and procedures must clearly state who should have access to what information and for what purposes. In addition, appropriate limitations must be placed on the collection, use and dissemination of clients and partners' personal and financial information and sufficient technological and administrative measures must be implemented to ensure the security of USDA data systems, processes and facilities.

All USDA employees are required to exhibit individual performance that reflects a commitment to dealing with every client and partner fairly and honestly and to respect the clients and partners' right to feel secure that their personal information is protected. To promote and maintain clients and partners' confidence in the privacy, confidentiality and security protections provided by the USDA, the USDA will be guided by the following Privacy Principles:

Principle 1:	Protecting citizen, client and partner privacy and safeguarding confidential citizen, client and partner information is a public trust.
Principle 2:	No information will be collected or used with respect to citizens, clients and partners that is not necessary and relevant for legally mandated or authorized purposes.
Principle 3:	Information will be collected, to the greatest extent practicable, directly from the citizen, client or partner to whom it relates.
Principle 4:	Information about citizens, clients and partners collected from third parties will be verified to the greatest extent practicable with the citizens, clients and partners themselves before action is taken against them.
Principle 5:	Personally identifiable citizen, client or partner information will be used only for the purpose for which it was collected, unless other uses are specifically authorized or mandated by law.
Principle 6:	Personally identifiable citizen, client or partner information will be disposed of at the end of the retention period required by law or regulation.

Principle 7:	Citizen, client or partner information will be kept confidential and will not be discussed with, nor disclosed to, any person within or outside the USDA other than as authorized by law and in the performance of official duties.
Principle 8:	Browsing, or any unauthorized access of citizen, client or partner information by any USDA employee, constitutes a serious breach of the confidentiality of that information and will not be tolerated.
Principle 9:	Requirements governing the accuracy, reliability, completeness, and timeliness of citizen, client or partner information will be such as to ensure fair treatment of all clients and partners.
Principle 10:	The privacy rights of citizens, clients and partners will be respected at all times and every citizen, client and partner will be treated honestly, fairly, and respectfully.

The Declaration does not, in itself, create any legal rights for clients and partners, but it is intended to express the full and sincere commitment of the USDA and its employees to the laws which protect client and partner privacy rights and which provide redress for violations of those rights.

APPENDIX B
POLICY STATEMENT ON CITIZEN, CLIENT AND PARTNER PRIVACY RIGHTS

The USDA is fully committed to protecting the privacy rights of all citizens, clients and partners. Many of these rights are stated in law. However, the USDA recognizes that compliance with legal requirements alone is not enough. The USDA also recognizes its social responsibility which is implicit in the ethical relationship between the USDA and the citizen, client or partner. The components of this ethical relationship are honesty, integrity, fairness, and respect.

Among the most basic of a citizens, clients, or partners' privacy rights is an expectation that the USDA will keep personal and financial information confidential. Citizens, clients and partners also have the right to expect that the USDA will collect, maintain, use, and disseminate personally identifiable information and data only as authorized by law and as necessary to carry out agency responsibilities.

The USDA will safeguard the integrity and availability of citizens, clients and partners' personal and financial data and maintain fair information and record keeping practices to ensure equitable treatment of all citizens, clients and partners. USDA employees will perform their duties in a manner that will recognize and enhance individuals' rights of privacy and will ensure that their activities are consistent with law, regulations, and good administrative practice. In our record keeping practices, the USDA will respect the individual's exercise of his/her First Amendment rights in accordance with law.

As an advocate for privacy rights, the USDA takes very seriously its social responsibility to citizens, clients and partners to limit and control information usage as well as to protect public and official access. In light of this responsibility, the USDA is equally concerned with the ethical treatment of citizens, clients and partners as well as their legal and administrative rights.